

Cursos, soluções e serviços baseados em software livres e padrões abertos para ambientes de missão crítica

▪*Experiência em missão crítica*

▪*Pioneira no ensino de Linux à distância*

▪*Parceira de treinamento IBM*

▪*Primeira com LPI no Brasil*

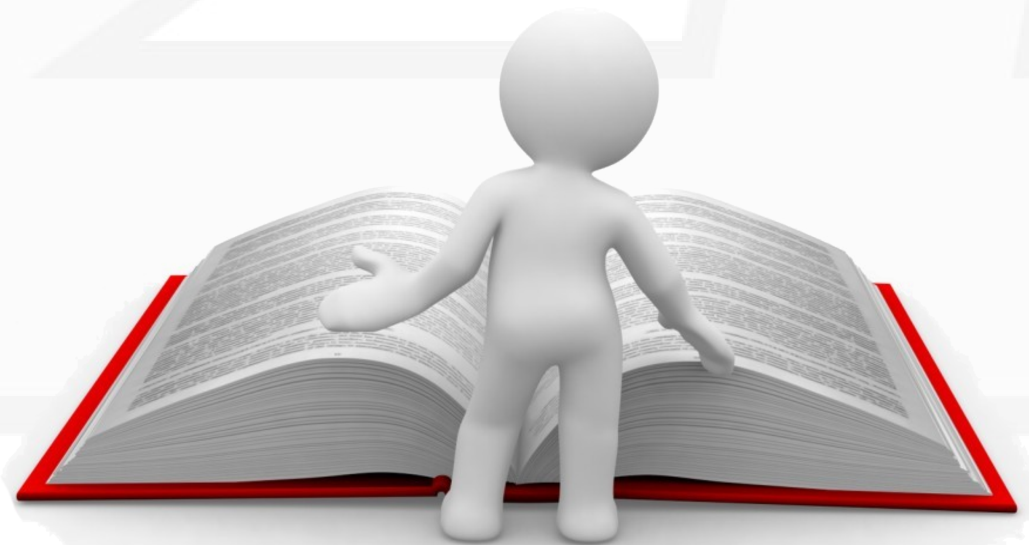
▪*+ de 30.000 alunos satisfeitos*

▪*Reconhecimento internacional*

▪*Inovação com Hackerteen e Boteconet*



Debian 6: Instalação e Hardening



No final da palestra

4LINUX
FREE SOFTWARE SOLUTIONS

➔ **As 05 primeiras perguntas ganharão um botton do tux.**

➔ **Sorteio do curso: 457 – Linux Network Servers**

- Preencham o cupom que está no folheto que vocês receberam na entrada da palestra;
- Se você já preencheu, ele já está aqui na urna
- O ganhador deve estar presente até o quinto sorteio. Se não estiver presente ganhará o sexto sorteado

Oportunidades

4LINUX
FREE SOFTWARE SOLUTIONS

- Apertar parafusos é fácil. Saber qual apertar poucos sabem.
- Existem poucos profissionais qualificados no mercado.
- Cada vez mais empresas adotam software livre.

Será que basta instalar uma distribuição linux para criar um servidor?



Antes da Instalação

FREE SOFTWARE SOLUTIONS

Planejamento:

- Quais serviços serão instalados?
- Quantos usuários?
- Qual a média de acesso?
- Pensar em redundância!!



Hardening na instalação

- **Particionamento**
  - /boot
  - /
  - /home
  - /usr
  - /var
  - /var/log
  - /tmp
  - swap –> preferencialmente SSD

- Para evitar qualquer problema com tamanho de partições use **LVM!!!**

Hardening na instalação

4LINUX
FREE SOFTWARE SOLUTIONS

• Implementar **RAID** para espelhamento (Redundância!!!)

• **Senha segura** para o root/usuário principal

• Desabilitar na BIOS o que não será utilizado:
  Portas Seriais
  Portas Paralelas
  Floppy Disk

Hardening no Sistema

4LINUX
FREE SOFTWARE SOLUTIONS

Os pacotes precisam vir de uma fonte segura:

vi /etc/apt/sources.list

deb http://ftp.br.debian.org/debian/ **squeeze** main

Para garantir que a fonte é segura:
apt-get install debian-keyring

Hardening no Sistema

Se quiser utilizar o sudo, cuidado!

```
# aptitude install sudo
# vi /etc/sudoers
usuario   ALL=(ALL) ALL
```

Os demais usuários do sistema não devem ter acesso ao sudo!!

Hardening no Sistema

4LINUX
FREE SOFTWARE SOLUTIONS

Desabilitar terminais para agilizar boot:

```
# vi /etc/inittab
```

1:2345:respawn:/sbin/getty 38400 **tty1**
2:23:respawn:/sbin/getty 38400 **tty2**
3:23:respawn:/sbin/getty 38400 **tty3**
4:23:respawn:/sbin/getty 38400 tty4
5:23:respawn:/sbin/getty 38400 tty5
6:23:respawn:/sbin/getty 38400 tty6

Hardening no Sistema

4LINUX
FREE SOFTWARE SOLUTIONS

Ainda no /etc/inittab:

ca:12345:ctrlaltdel:/sbin/shutdown -t1 -a -r now

Comentar ou modificar a ação!

Exemplo:
ca:12345:ctrlaltdel:/bin/echo “Você pressionou Control+Alt+Del”

Hardening no Sistema

4LINUX
FREE SOFTWARE SOLUTIONS

Alteração do uso da swap (se necessário):

```
# cat /proc/sys/vm/swappiness

# echo 'vm.swappiness = 0' >> /etc/sysctl.conf
```

Hardening no Sistema

4LINUX
FREE SOFTWARE SOLUTIONS

Verificar serviços de rede com netstat:
netstat -nltup

Hardening no Sistema

4LINUX
FREE SOFTWARE SOLUTIONS

Remover pacotes desnecessários:

aptitude remove --purge bsd-mailx exim4 exim4-base exim4-config exim4-daemon-light mutt procmail telnet

Hardening no Sistema

4LINUX
FREE SOFTWARE SOLUTIONS

Apagar pacotes órfãos de sistema:

```
# aptitude install deborphan
# deborphan | xargs apt-get -y remove --purge
```

Hardening no Sistema

Cuidados as opções de montagem do /etc/fstab:

...

/dev/sda2 /home ext4 **defaults,noexec,nodev** 0 0
/dev/sda3 /tmp ext4 **defaults,noexec,nodev** 0 0

...

Hardening no Sistema

Atribuir logout automático:

```
# vi /etc/profile
TMOUT=1200
HISTSIZE=100
```

Hardening no Sistema

4LINUX
FREE SOFTWARE SOLUTIONS

Ao instalar o SSH Server para manutenção remota:

```
# vi /etc/ssh/sshd_config
```

```
Port 2222
PermitRootLogin no
LoginGraceTime 30
IdleTimeout 15m
Forward X11 no
AllowUsers usuario1 usuario2
```

Hardening no Sistema

FREE SOFTWARE SOLUTIONS

Limitando o acesso de root:

vi /etc/securetty
...
tty1
tty2
tty3
tty4
tty5
...

Hardening no Sistema

4LINUX FREE SOFTWARE SOLUTIONS

Utilize o PAM como seu aliado!

Limitando o uso de memória e cpu dos usuários, evitamos o famoso forkbomb:

:(){ :|: & };:

Hardening no Sistema

Por padrão, qual o número máximo de processos que podem ser executados ao mesmo tempo?

root@debian:/# **ulimit -u**
unlimited

Qual o tempo máximo de uso de cpu?

root@debian:/# **ulimit -t**
unlimited

Qual o tamanho máximo de arquivo que os usuários podem criar?

root@debian:/# **ulimit -f**
unlimited

Hardening no Sistema

FREE SOFTWARE SOLUTIONS

Limitando usuários:

vim /etc/security/limits.conf

<usuario/grupo> <tipo_de_limite> <recurso> <valor_do_limite>

*	hard	nproc	100
*	hard	cpu	480
*	hard	fsize	100000
*	hard	maxlogins	2
*	hard	rss	100000

Hardening no Sistema

4LINUX
FREE SOFTWARE SOLUTIONS

Ainda no PAM podemos limitar o acesso dos usuários por horário:

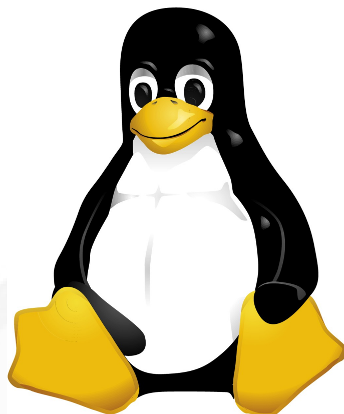
```
# vi /etc/pam.d/login
account   requisite  pam_time.so

# vi /etc/security/time.conf
serviços;ttys;usuários;horario

login;*;root;Al0600-2200
sshd:*:bruna:Wd2100-2400
```

Obrigado

FREE SOFTWARE SOLUTIONS



Bruna Griebeler
bruna@4linux.com.br
www.4linux.com.br
www.hackerteen.com
twitter.com/4LinuxBR

Tel: 55-11-2125-4747